What is claimed is:

1. A qualification authentication method using variable authentication information, comprising an first-time registration phase and an authentication phase;

the first-time registration phase includes:

a step in which a person to be authenticated generates first-time authentication data by using a one-way function which generates output one-way information which makes it difficult to calculate input information in terms of computational complexity, based on an own user ID, password and a random number;

a step in which the person to be authenticated transmits an own user ID and the first-time authentication data to the authenticating person; and

a step in which the authenticating person registers the first-time authentication data received from the person to be authenticated as an authentication parameter used at the time of first-time authentication; and

the authentication phase includes:

a step in which the person to be authenticated generates, intermediate data for this time authentication data, this time authentication data, next time authentication data, and an intermediate parameter for certification of authentication, using the one-way function based on the own user ID, password and a random number; and performs an exclusive OR operation using the this time authentication data and the intermediate parameter for certification of authentication, with respect to the intermediate data for this time authentication data, and an exclusive OR operation using the this time authentication data with respect to the next time authentication data, to thereby generate an exclusive OR for this time authentication and an exclusive OR for next time authentication;

a step in which the person to be authenticated transmits the own user ID, the exclusive OR for this time authentication and the exclusive OR for next time authentication to the authenticating person;

a step in which the authenticating person generates a temporary parameter for next time certification based on the exclusive OR of the exclusive OR for next time authentication received from the person to be authenticated and the authentication parameter registered in the previous time, and generates an intermediate parameter for certification of authentication using the one-way function from the temporary parameter for next time authentication;

a step in which the authenticating person generates a validity confirmation parameter for the person to be authenticated, using the one-way function and designating, as the input information, an exclusive OR of the exclusive OR for this time authentication received from the person to be authenticated, the previously registered authentication parameter, and the intermediate parameter for certification of authentication, compares the validity confirmation parameter and the previously registered authentication parameter, and if these parameters agree with each other, the authenticating person judges that the authentication is approved, and if these parameters do not agree with each other, the authenticating person judges that the authentication is not approved; and

a step in which when the authentication is approved, the temporary parameter for next time authentication is registered as an authentication parameter for next time authentication instead of the previously registered authentication parameter.

2. A qualification authentication method according to claim 1, wherein a function for private key cryptography is used as the one-way function E.

3. A qualification authentication method according to claim 1, wherein DES or FEAL function is used as the one-way function E.